INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2001 - 2004

COM 11-R 8-E
January 2001
Original: English

Question: 13/11

Texte disponible seulement en
Text available only in
Texto disponible solamente en

STUDY GROUP 11 - REPORT R 8

SOURCE*: STUDY GROUP 11

TITLE: IMPLEMENTORS' GUIDE (12/2000) FOR RECOMMENDATION Q.2111 (12/99)

_____

1 Introduction

1.1 References

[1] ITU-T Recommendation Q.2111 (12/99): B-ISDN ATM Adaptation Layer - Service Specific Connection Oriented Protocol in a Multilink and Connectionless Environment (SSCOPMCE).

1.2 Background

This guide is a compilation of reported defects, their resolutions and minor upgrades to the 1999 edition of ITU-T Recommendation Q.2111 [1]. It includes all approved corrigenda and is intended to be an additional authoritative source of information for implementors to be read in conjunction with the Recommendation itself.

1.3 Scope of the guide

This guide records the resolutions of defects in the following categories:

- editorial errors;
- technical errors, such as omissions, inconsistencies, etc.; and
- ambiguities.

* **Contact:** Dr Pietro Schicker

Tel: +41 1 938 1555
Fax: +41 1 938 1557
E-mail: schicker@scicon.ch

In addition, this guide records minor enhancements to the Recommendation in the following categories:

- increased interoperability; and
- deployment possibly in new environments.

2 Editorial errors

None.

3 Technical errors

None.

4 Ambiguities

None.

5 Increased interoperability

None.

6 Deployment possibility in new environments

6.1

Deployment in IP networks offering Differentiated Services

a) Add the following reference to § 2.1 (Normative references):

[13] IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.

b) Add the following reference to § 2.2 (Bibliography):

[14] IETF RFC 2475, An Architecture for Differentiated Services.

c) Add an abbreviation to § 4 as follows:

DS Differentiated Services

d) Replace the last sentence in the paragraph after Figure 2/Q.2111 as follows:

Annexes C and D describe the mapping of primitives across this SAP with IP and UDP; Annex C covers legacy IP networks while Annex D covers IP networks that support differentiated services.

e) Replace the last sentence in § 7.3.3 (Connectionless environment) as follows:

Such functions for IP or UDP based communications are defined in Annexes C and D to this Recommendation.

f) Replace the note in Annex C (Convergence function for SSCOPMCE above IP or UDP) § C.1 (General description) as follows:

NOTE - The convergence function of this Annex, being based upon IETF RFC 791[8], is designed specifically for operation with IPv4. If use is desired of an application, e.g., the "Differentiated Services" defined in IETF RFC 2475, that is not compatible with IETF RFC 791[8], then this Annex is not applicable; for the application of "Differentiated Services" see Annex D.

g) Add the new Annex D (Convergence function for SSCOPMCE above IP or UDP with Differentiated Services) which is represented in Attachment A.

ATTACHMENT A

ANNEX D

Convergence function for SSCOPMCE above IP or UDP with Differentiated Services

D.1 General description

The convergence function for SSCOPMCE above IP provides for the possibility to deploy SSCOPMCE on top of the connectionless service provided by IP. The IP service utilizes protocol defined in IETF RFCs 791 [8], 1122 [10], in addition, the Differentiated Services Field is defined in IETF RFC 2474 [13]. Alternatively, UDP service, as defined in IETF RFC 768 [18], may be used. Both alternatives are discussed in this annex.

NOTE - The architecture of the differentiated service is described in IETF RFC 2475 [14].

All protocol stacks that include SSCOPMCE can, therefore, also be used in IP-based networks that deploy the differentiated service. A particular application of this arrangement is a protocol stack for SS No. 7 signalling.

D.2 Functions of the convergence function

The purpose of the convergence function is to map information between SSCOPMCE and IP (or UDP) PDUs. Appropriate headers must be created as is customarily done in the IP (or UDP) environment.

D.3 Specification of the convergence function

Clause 7.3/Q.2111 defines the primitives and parameters used at the lower boundary of the SSCOPMCE protocol entity. It shows that the parameters of the CPCS-UNITDATA.invoke primitive are used to model the transfer of information from SSCOPMCE protocol entity to the entity serving it. It also shows that the parameters of the CPCS-UNITDATA.signal primitive are used to model the transfer of information from the entity serving the SSCOPMCE protocol entity to that SSCOPMCE protocol entity.

D.3.1 The IP interface to its users

D.3.1.1 Description of the IP upper interface

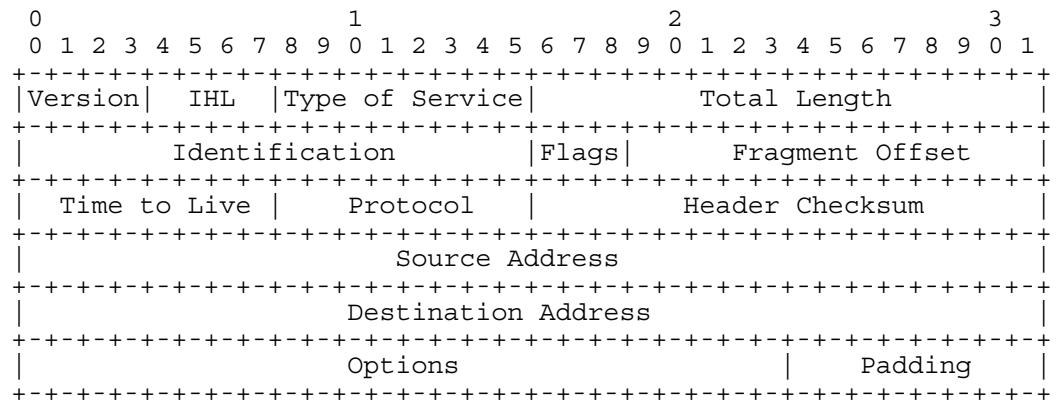
The user interface to the IP is described by example in IETF RFC 791 [8] in a quasi-formal way through the exchange of "SEND" and "RECEIVE" primitives (although the language is modelled on descriptions of function calls in an operating system). All IP implementations must provide a certain minimum set of services to guarantee that all IP implementations can support the same protocol hierarchy.

Since Internet protocol is a datagram protocol, there is minimal memory or state maintained between datagram transmissions, and each call on the Internet protocol module by the user supplies all information necessary for the IP to perform the service requested.

When the user sends a datagram, it transmits the SEND primitive, supplying all the arguments. The Internet protocol module, on receiving this primitive, checks the arguments and prepares and sends the message. If either the arguments are bad, or the network does not accept the datagram, a reasonable report must be made to the user as to the cause of the problem, but the details of such reports are up to individual implementations.

When a datagram arrives at the Internet protocol module from the network, the information contained in the datagram is passed from the datagram to the user. If the user addressed does not exist, an ICMP error message is returned to the sender and the data is discarded, as described in IETF RFCs 792 [9] and 1122 [10].

IETF RFC 791 [8] defines the contents of the IP packet header as shown in Figure D.1/Q.2111.



NOTE - Each tick mark represents one bit position.

FIGURE D.1/Q.2111

Example Internet Datagram Header

The fields of the header shown in Figure D.1/Q.2111 are defined in RFC 791 [8] as follows:

Version (4 bits)

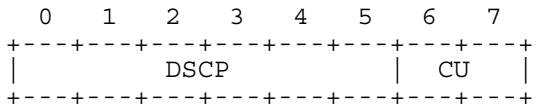
The Version field indicates the format of the Internet header.

IHL (4 bits)

Internet Header Length is the length of the Internet header in 32 bit words, and thus points to the beginning of the data. Note that the minimum value for a correct header is 5.

Type of Service (8 bits)

When IPv4 is deployed on a network supporting the differentiated services, this field is used as the differentiated services field (DS field) as defined in IETF RFC 2474 [14]. The DS field structure is defined as follows:



DSCP: Differentiated Services Codepoint
Six bits of the DS field are used as a codepoint (DSCP) to select the per-hop behaviour a packet experiences at each node.

CU: Currently Unused
A two-bit currently unused (CU) field is reserved and its definition and interpretation are outside the scope of this document. The value of the CU bits are ignored by differentiated services-compliant nodes when determining the per-hop behaviour to apply to a received packet.

A specification of the packet forwarding treatments selected by the DS field values of "xxx000|xx", or DSCP = "xxx000" and CU subfield unspecified, are reserved as a set of Class Selector Codepoints. per-hop behaviours which are mapped to by these codepoints MUST satisfy the Class Selector per-hop behaviour requirements in addition to preserving the default per-hop behaviour requirement on codepoint "000000". In IETF RFC 2474 [13], the meaning of the "Class Selector Codepoint" is defined as follows:

> To preserve partial backwards compatibility with known current uses of the IP Precedence field without sacrificing future flexibility, we have taken the approach of describing minimum requirements on a set of per-hop behaviours that are compatible with most of the deployed forwarding treatments selected by the IP Precedence field. In addition, we give a set of codepoints that MUST map to per-hop behaviours meeting these minimum requirements. The per-hop behaviours mapped to by these codepoints MAY have a more detailed list of specifications in addition to the required ones stated here. Other codepoints MAY map to these same per-hop behaviours. We refer to this set of codepoints as the Class Selector Codepoints, and the minimum requirements for per-hop behaviours that these codepoints may map to are called the Class Selector per-hop behaviour Requirements.

The Precedence Field is defined in IETF RFC 791 [8] as follows:

Precedence
111 Network Control
110 Internetwork Control
101 CRITIC/ECP
100 Flash Override
011 Flash
010 Immediate
001 Priority
000 Routine

Total Length (16 bits)

Total Length is the length of the datagram, measured in octets, including Internet header and data. This field allows the length of a datagram to be up to 65 535 octets.

NOTE - The maximal Internet header is 60 octets, and a typical Internet header is 20 octets.**Identification** (16 bits)

An identifying value assigned by the sender to aid in assembling the fragments of a datagram.

Flags (3 bits)

Various Control Flags.

Bit 0 reserved, must be zero

Bit 1 (DF) 0 = May Fragment, 1 = Don't Fragment.

Bit 2 (MF) 0 = Last Fragment, 1 = More Fragments.

Fragment Offset (13 bits)

This field indicates where in the datagram this fragment belongs. The fragment offset is measured in units of 8 octets (64 bits). The first fragment has offset zero.

Time to Live (8 bits)

This field indicates the maximum time the datagram is allowed to remain in the Internet system. If this field contains the value zero, then the datagram must be destroyed by an intermediate host (but not by the destination host). This field is modified in Internet header processing. The time is measured in units of seconds, but since every module that processes a datagram must decrease the TTL by at least one even if it processes the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram may exist. The intention is to cause undeliverable datagrams to be discarded, and to bound the maximum datagram lifetime.

Protocol (8 bits)

This field indicates the next level protocol used in the data portion of the Internet datagram. The values for various protocols are specified by the IETF. The numeric value for SSCOPMCE is "128".

Header Checksum (16 bits)

A checksum on the header only. Since some header fields change (e.g., time to live), this is recomputed and verified at each point that the Internet header is processed.

The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.

Source Address (32 bits)

The source address. See section 3.2/IETF RFC 791 [8].

Destination Address (32 bits)

The destination address. See section 3.2/IETF RFC 791 [8].

Options (variable)

The options may appear or not in datagrams. They must be implemented by all IP modules (host and gateways). What is optional is their transmission in any particular datagram, not their implementation.

In some environments the security option may be required in all datagrams.

The option field is variable in length. There may be zero or more options. The specific coding of the options field may be found in IETF RFC 791 [8].

D.3.1.2 Transmitter Side Mapping

Figure D.2/Q.2111 shows the Service Data Unit and Parameters passed between the SSCOPMCE/Convergence Function and the IP layer at the transmitting side. In this figure, it can be seen that the relevant fields of the IP packet header should be coded as shown in Table D.1/Q.2111.

D.3.1.3 Receiver Side Mapping

Figure D.3/Q.2111 shows the Service Data Unit and Parameters passed between SSCOPMCE/Convergence Function and the IP layer at the receiving side.

TABLE D.1/Q.2111

Transmitter side mapping

Version	(NOTE 1)	
Internet Header Length (IHL)	(NOTE 1)	
Differentiated Services Field (NOTE 5)	00000000	If "Cell Loss Priority" = 1
	(NOTE 6)	If "Cell Loss Priority" = 0
Total Length (TL)	(NOTE 1)	
Identification	(NOTE 2)	
Flags	000	May fragment; last fragment
	001	May fragment; more fragments
Fragment Offset	(NOTE 1)	
Time to Live (TTL)	(NOTE 2)	
Protocol (PROT)	(NOTE 2)	"128"
IP Header Checksum	(NOTE 1)	
Source Address	(NOTE 2)	the IP address of the source node
Destination Address	(NOTE 2)	the IP address of the destination node
Options	(NOTE 1)	(NOTE 4)
Data	(NOTE 3)	1 to (65 535 - IHL)

NOTE 1 - Coding of this parameter is handled by the IP module using guidance provided in IETF RFC 791 [8].

NOTE 2 - Coding of this parameter is handled by the convergence function using the rules specified in IETF RFC 791 [8].

NOTE 3 - The SSCOP-PDU is appended with the CPCS-PDU trailer, coded as specified in I.363.5 [14].

NOTE 4 - For the purpose of this Recommendation, the user options "Loose Source and Record Route," "Strict Source and Record Route," "Record Route," and "Timeshare" apply. Other user options shall not be used and shall be silently ignored when received (see IETF RFC 1122 [10] section 3.2.1.8). It should be noted that the options "No Operation" (Type 1) and "End of List" (Type 0) are to be handled within the IP module; therefore, they are not passed to the transport layer.

NOTE 5 - A replacement header field, called the DS field, is defined, which is intended to supersede the existing definitions of the IPv4 TOS octet (see RFC 791 [8]).

NOTE 6 - This field should be set to a value representing the quality equal to "Cell Loss Priority = 0". Therefore, the first three bits should be greater than "000", e.g., "11100000" in a network where it is appropriate.

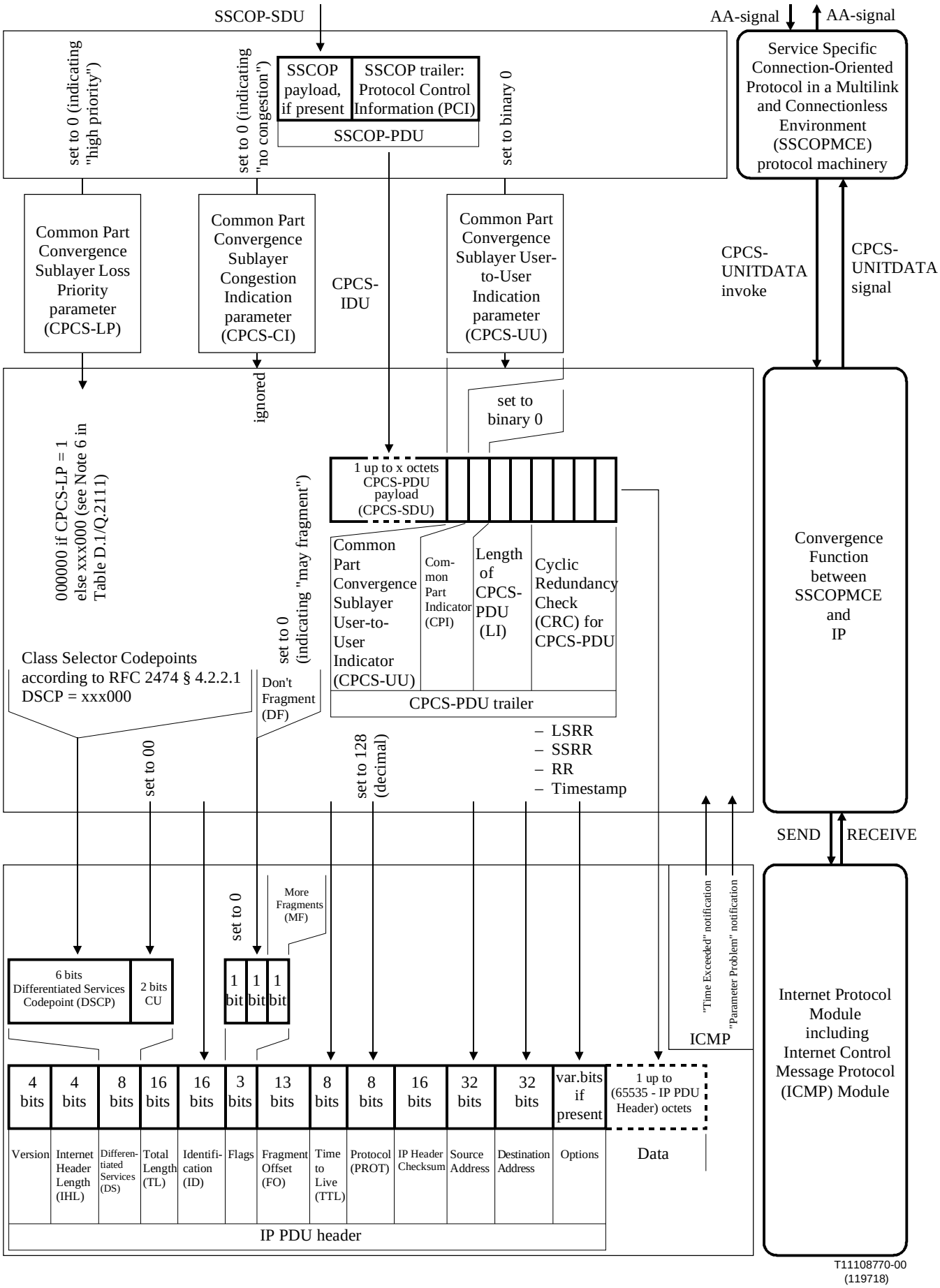


FIGURE D.2/Q.2111

Service Data Unit and Parameters passed between SSCOPMCE/ Convergence Function and IP Layer - Transmitting side

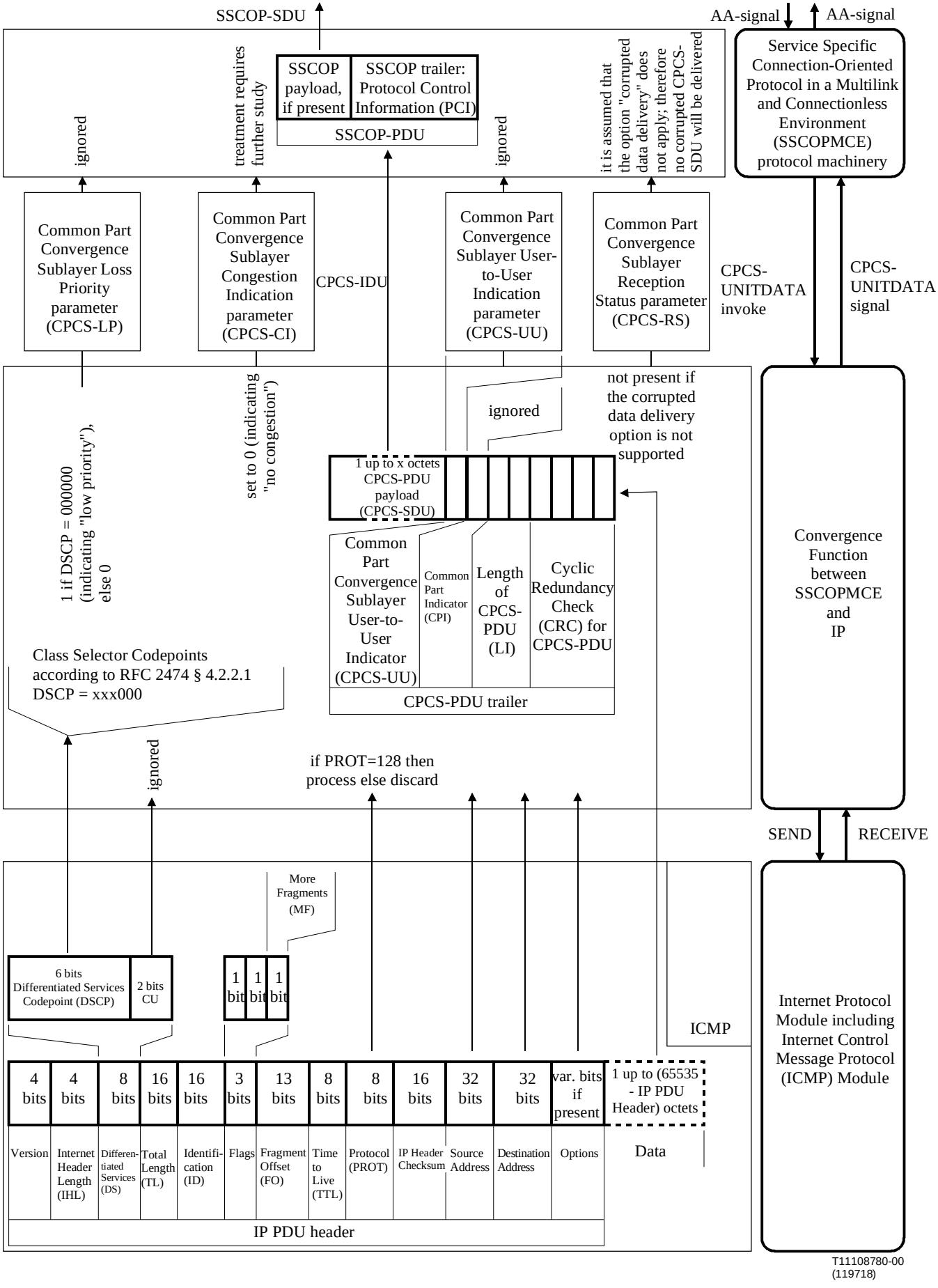


FIGURE D.3/Q.2111

Service Data Unit and Parameters passed between SSCOPMCE/ Convergence Function and IP Layer - Receiving side

Figure legend to Figure D.2	**Figure legend to Figure D.3**
1 Precedence	1 Precedence
2 Delay (D)	2 Delay (D)
3 Throughput (T)	3 Throughput (T)
4 Reliability (R)	4 Reliability (R)
5 Monetary Cost (MC)	5 Monetary Cost (MC)
6 Don't Fragment (DF)	6 Common Part Indicator (CPI)
7 Common Part Indicator (CPI)	7 More Fragments (MF)
8 More Fragments (MF)	8 Version
9 "Time Exceeded" notification	9 Internet Header Length (IHL)
10 "Parameter Problem" notification	10 Type of Service (TOS)
11 Version	11 Total Length (TL)
12 Internet Header Length (IHL)	12 Identification (ID)
13 Type of Service (TOS)	13 Flags
14 Total Length (TL)	14 Fragment Offset (FO)
15 Identification (ID)	15 Time to Live (TTL)
16 Flags	16 Protocol (PROT)
17 Fragment Offset (FO)	17 IP Header Checksum
18 Time to Live (TTL)	18 Source Address
19 Protocol (PROT)	19 Destination Address
20 IP Header Checksum	20 Options
21 Source Address	
22 Destination Address	
23 Options	

D.3.2 The UDP interface to its users

D.3.2.1 Description of the UDP upper interface

IETF RFC 768 [7] defines the parameters of the UDP packet header as shown in Figure D.4/Q.2111.

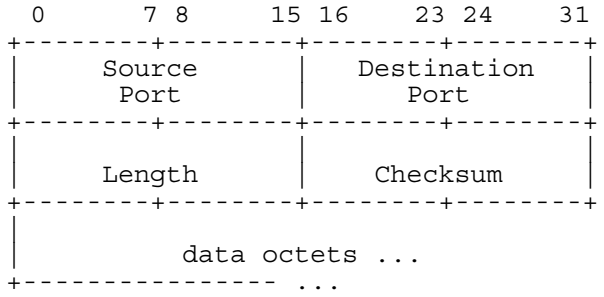


FIGURE D.4/Q.2111

UDP Header Format

The fields of the header shown in Figure D.4/Q.2111 are defined in RFC 768 [7] as follows:

Source Port (16 bits)

Source Port is an optional field, when meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

Destination Port (16 bits)

Destination Port has a meaning within the context of a particular Internet destination address.

Length (16 bits)

Length is the length in octets of this user datagram including this header and the data. (This means the minimum value of the length is eight.)

Checksum (16 bits)

Checksum is the 16-bit one's complement of the one's complement sum of a pseudo-header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

The pseudo-header conceptually prefixed to the UDP header contains the source address, the destination address, the protocol, and the UDP length. This information gives protection against misrouted datagrams. This checksum procedure is the same as is used in TCP.

NOTE - For the purpose of this recommendation the source address, the destination address, and the protocol are modelled as parameters.

D.3.2.2 Transmitter Side Mapping

Figure D.5/Q.2111 shows the Service Data Unit and Parameters passed between the SSCOPMCE/Convergence Function and the UDP and IP modules at the transmitting side.

D.3.2.3 Receiver Side Mapping

Figure D.6/Q.2111 shows the Service Data Unit and Parameters passed between the SSCOPMCE/Convergence Function and the UDP and IP modules at the receiving side.

D.4 Layer Management

There are no interactions with layer management defined.

It is for further study whether there exists a need for the Convergence Function to invoke the services of the Internet Control Message Protocol (ICMP) to notify the peer of error situations, such as Protocol Unreachable and Port Unreachable, in the absence of a peer-to-peer mechanism (see IETF RFC 1122 [10] section 3.2.2.1).

It is for further study whether SSCOPMCE should provide positive and/or negative advice to modify the routing of messages upon "Dead Gateway Detection" (see IETF RFC 1122 [10] section 3.3.1.4).

Figure legend to Figure D.5	**Figure legend to Figure D.6**
1 Precedence	1 Precedence
2 Delay (D)	2 Throughput (T)
3 Throughput (T)	3 Reliability (R)
4 Reliability (R)	4 Monetary Cost (MC)
5 Monetary Cost (MC)	5 Destination Port
6 Destination Port	6 More Fragments (MF)
7 More Fragments (MF)	7 Version
8 "Time Exceeded" notification	8 Internet Header Length (IHL)
9 "Parameter Problem" notification	9 Type of Service (TOS)
10 Var. bits if present	10 Total Length (TL)
11 Version	11 Identification (ID)
12 Internet Header Length (IHL)	12 Flags
13 Type of Service (TOS)	13 Fragment Offset (FO)
14 Total Length (TL)	14 Time to Live (TTL)
15 Identification (ID)	15 Protocol (PROT)
16 Flags	16 IP Header Checksum
17 Fragment Offset (FO)	17 Sourace Address
18 Time to Live (TTL)	18 Destination Address
19 Protocol (PROT)	19 Options
20 IP Header Checksum	
21 Source Address	
22 Destination Address	
23 Options	

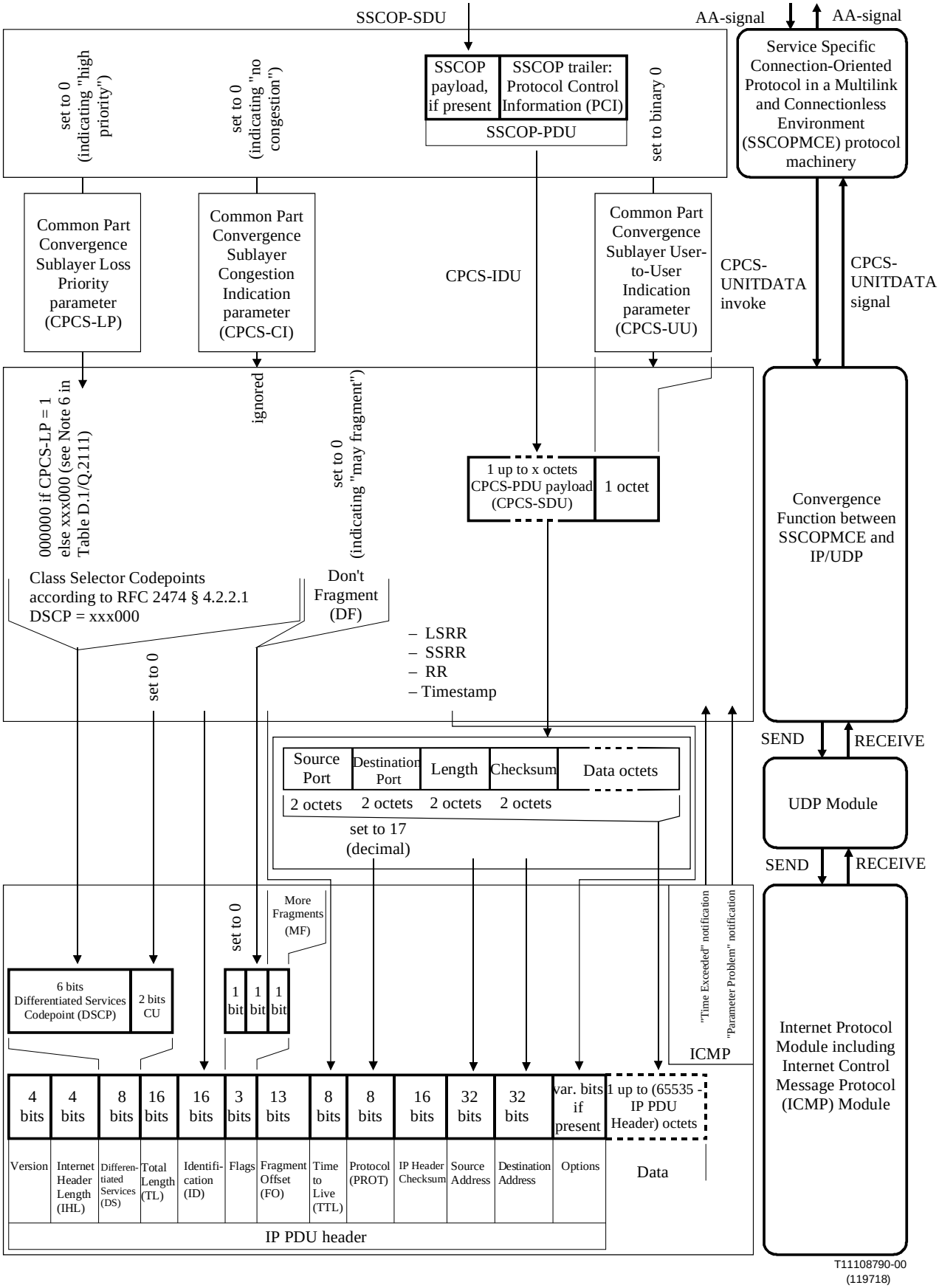


FIGURE D.5/Q.2111

Service Data Unit and Parameters passed between SSCOPMCE/ Convergence Function and UDP/IP Layer - Transmitting side

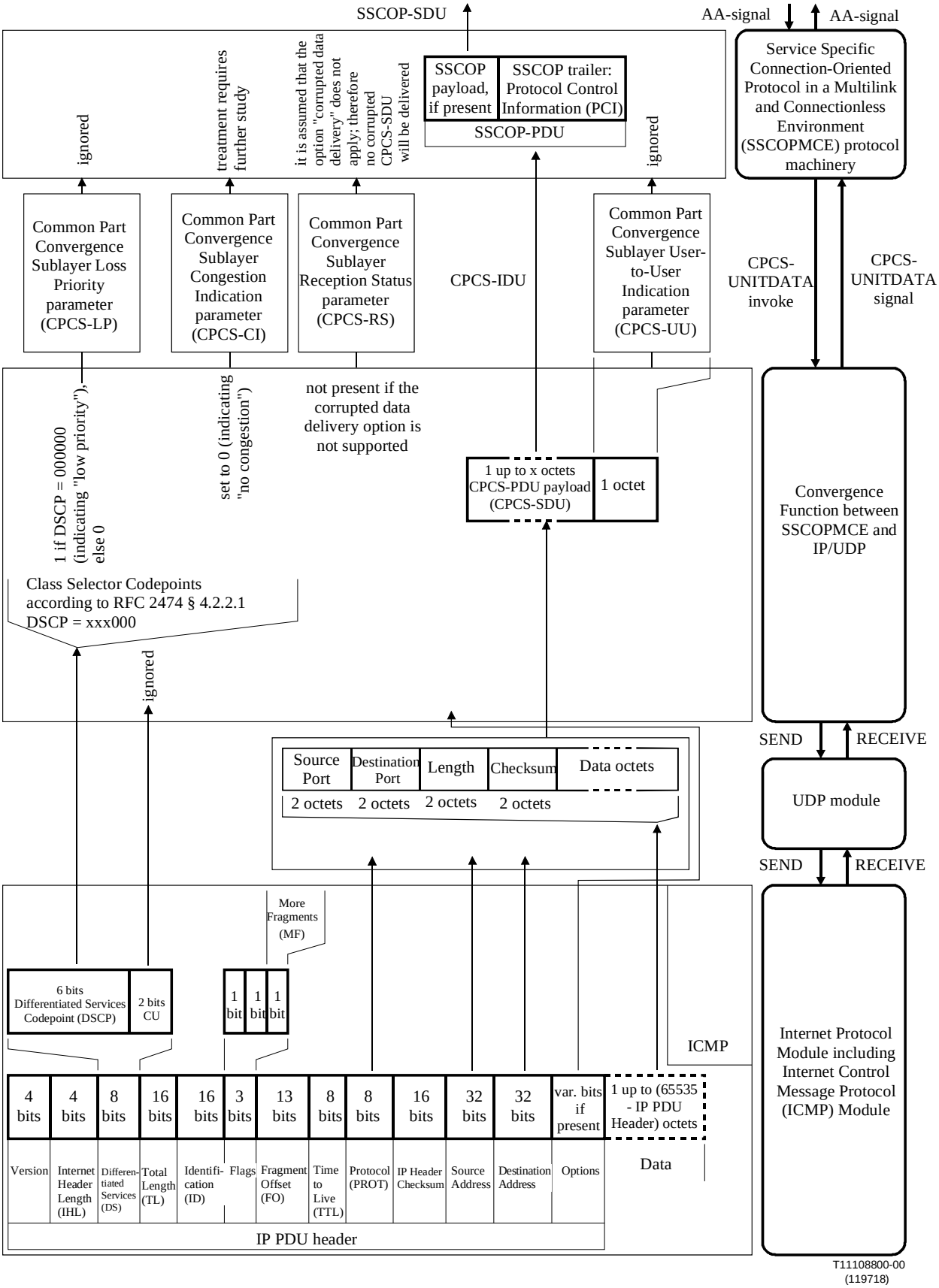


FIGURE D.6/Q.2111

Service Data Unit and Parameters passed between SSCOPMCE/Convergence Function and UDP/IP Layer - Receiving side